대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0017022
Application Number

출 원 년 월 일 : 2003년 03월 19일
Date of Application MAR 19, 2003

출 원 인 : 학교법인 한국정보통신학원
Applicant(s) INFORMATION AND COMMUNICATIONS UNIVERSITY EDUCATION/

2003 년 06 월 04 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0003
【제출일자】	2003.03.19
【발명의 명칭】	네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법
【발명의 영문명칭】	ANONYMOUS FINGERPRINTING SCHEME BASED ON THE BILINEAR PAIRINGS DIFFIE-HELLMAN PROBLEM
【출원인】	
【명칭】	학교법인 한국정보통신학원
【출원인코드】	2-1999-038195-0
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2000-005740-6
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2000-005743-8
【발명자】	
【성명의 국문표기】	김명선
【성명의 영문표기】	KIM,Myungsun
【주민등록번호】	700521-1478511
【우편번호】	305-732
【주소】	대전광역시 유성구 화암동 58-4
【국적】	KR
【발명자】	
【성명의 국문표기】	김광조
【성명의 영문표기】	KIM,Kwangjo
【주민등록번호】	560410-1347622

【우편번호】	305-732
【주소】	대전광역시 유성구 화암동 58-4
【국적】	KR
【공개형태】	학술단체 서면발표
【공개일자】	2002.12.16
【심사청구】	청구
【조기공개】	신청
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 심사청구 , 특허법 제64조의 규정에 의한 출원공개를 신청합니다. 대리인 장성구 (인) 대리인 김원준 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	1	면	1,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	6	항	301,000 원
【합계】	331,000 원		
【감면사유】	학교		
【감면후 수수료】	165,500 원		

【첨부서류】 1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_1통 3.고등교육법 제2조에의한 학교임을 증명하는 서류[설립인가서]_1통

【요약서】

【요약】

본 발명은 구매자의 신분 정보를 누출시키지 않고 디지털 정보의 지적 재산권을 보호하는데 적합한 네트워크상에서의 겹선형쌍 디피-헬만 문제(Bilinear Diffie-Hellman Problem)를 이용한 익명 핑거프린팅(Fingerprinting) 방법에 관한 것이다.

영지식 증명이나 그룹서명에 기반을 두고 있는 기존 익명 핑거프린팅 기법은 그 연산 과정이 복잡하고 참여 개체 키의 크기가 지나치게 길기 때문에 실용적이지 못하다는 문제가 제기되었다.

본 발명에서는 겹선형 쌍을 이용하여 각 개체의 연산 능력이 낮은 경우를 고려하여 효율적인 연산을 가능하게 하고, 특히 키 크기가 작으면서도 안전한 익명 핑거프린팅 기법을 설계하고자 한다.

【대표도】

도 2

【명세서】

【발명의 명칭】

네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법

{ANONYMOUS FINGERPRINTING SCHEME BASED ON THE BILINEAR PAIRINGS DIFFIE-HELLMAN PROBLEM}

【도면의 간단한 설명】

도 1은 본 발명을 구현하기 위한 핑거프린팅 참여자간의 상호작용 구성도,

도 2는 본 발명의 바람직한 실시예에 따른 익명 핑거프린팅 과정의 전체 흐름도,

도 3a는 도 2의 구매자 등록 과정의 상세 흐름도,

도 3b는 도 2의 판매자가 구매자를 인증하는 과정의 상세 흐름도,

도 3c는 도 2의 구매자와 판매자간의 지문삽입 과정의 상세 흐름도,

도 3d는 도 2의 판매자와 신뢰기관간의 불법 구매자 판별 과정의 상세 흐름도.

<도면의 주요부분에 대한 부호의 설명>

100 : 구매자 200 : 판매자

300 : 키생성 센터 또는 신뢰기관

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<10> 본 발명은 네트워크상에서 디지털 상품이나 전자도서와 같은 디지털 지적재산의 불법 복사 및 배포를 방지하기 위한 기술에 관한 것으로, 특히, 겹선형 쌍(Bilinear

Pairings)을 이용하여 안전하고 효율적인 익명 핑거프린팅(fingerprinting) 기법을 제공하는데 적합한 네트워크상에서의 겹선형쌍 디피-헬만 문제(Diffie-Hellman problem)를 이용한 익명 핑거프린팅 방법에 관한 것이다.

<11> 컴퓨터 네트워크의 발전과 인터넷의 급속한 보급으로 인해 디지털화된 저장 정보의 보호가 매우 중요한 사안으로 대두되었다.

<12> 이를 위해, 디지털 데이터의 지적 재산권의 기술적 보호 방법을 설계하기 위한 다양한 연구들이 진행되었는데, 그 대표적인 연구 결과로서 핑거프린팅 기법과 워터마킹(Water-marking) 기법을 예로 들 수 있다.

<13> 워터마킹 기법은 불법 복사 방지 및 소유권 증명의 합리적 대안으로서, 디지털 재산의 소유주가 디지털 정보에 특정 데이터를 삽입하고 추출할 수 있는 기술을 일컫는다. 반면, 핑거프린팅 기법은 구매자가 자신과 관련된 특정 정보를 삽입하고, 불법적으로 유포된 사본으로부터 불법 구매자 또는 불법 배포자를 판매자가 추적할 수 있게 하는 기술이다.

<14> 통상, 핑거프린팅 기법은 두 종류로 구분되는데, 하나는 대칭형(symmetric) 핑거프린팅 기법이며, 다른 하나는 비대칭형(asymmetric) 핑거프린팅 기법이다.

<15> 대칭형 핑거프린팅 기법은 블레이클리(Blakley), 메도우(Meadows) 및 퍼디(Purdy)에 의해서 제안되어 보네(Boneh)와 쇼(Shaw)에 의해서 발전하였고, 비대칭형 핑거프린팅 기법은 피츠먼(Pfitzmann)에 의해서 제안되고 발전하였다.

<16> 대칭형 핑거프린팅 기법에서는 상인이 지문(fingerprint)이라는 특수한 정보를 삽입하는 반면, 비대칭형 핑거프린팅 기법에서는 구매자와 판매자 사이의 대화형 프로토콜

을 사용하여 구매자가 추후 불법 구매자를 확인하기 위한 목적에만 사용되는 고유 정보인 지문을 삽입시킨다.

<17> 결국, 삽입된 지문이 개인을 식별하기 위한 고유한 정보로 사용될 수 있다는 점에서 일맥상통하지만, 비대칭형 기법은 상인이 직접 지문 정보를 추출하여 불법 구매자가 누구인지 제3자, 특히 신뢰기관을 설득시킬 수 있다는 점에서 대칭형 기법과 대비된다.

<18> 그러나, 상술한 두 가지 기법은, 양자 공히 구매자의 신원 정보가 쉽게 누출될 수 있다는 단점이 있다. 특히 개방 네트워크상에서 디지털 정보를 구매하는 과정에서는 구매자의 구매 행위에 대한 정보가 누출될 수 있으며, 이렇게 누출된 정보는 불법적으로 악용될 수 있다.

<19> 이러한 문제를 해결하기 위한 종래의 일환으로, 익명(Anonymous) 비대칭 핑거프린팅 기법(이하, 익명 핑거프린팅 기법이라 약칭함)이 피츠먼과 와이드너(Waidner)에 의해 제안되었으며, 이후 대화식 영지식 증명이나 그룹 서명 기법을 이용한 다수의 익명 핑거프린팅 기법들이 제안되었다.

<20> 그러나, 이러한 기존 기법들의 대부분은 구매자의 연산 능력의 다양성을 고려하지 않았다. 즉, 구매자의 연산 능력이 우수한 경우에는 기존 기법의 적용이 가능하나, 구매자의 연산 능력이 낮은 경우에는 그 적용이 불가능하였다.

<21> 특히, 기존 기법들에서 제시된 과도한 키의 크기는 실용적 적용을 불가능하게 하는 계기가 되었다.

<22> 따라서, 모든 연산이 효율적으로 수행되고, 특히 키의 크기 측면에서 실용적으로 활용될 수 있는 익명 핑거프린팅 기술이 요망된다.

【발명이 이루고자 하는 기술적 과제】

<23> 본 발명은 상술한 요망에 의해 안출한 것으로, 베일쌍(Weil pairings)이나 테이트(Tate)쌍과 같은 겹선형쌍을 익명 핑거프린팅 기법에 적용하여 네트워크상의 불법 구매자를 판별함으로써, 키 크기를 줄이고 연산 효율성을 극대화하도록 한 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법을 제공하는데 그 목적이 있다.

<24> 이러한 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따르면, 신뢰기관에서 시스템 매개변수를 설정하고 각 개체의 공개키와 비밀키를 생성하는 단계와; 공개키와 비밀키를 이용하여 구매자측 단말을 통해 임의 구매자의 정보를 신뢰기관에 등록하는 단계와; 판매자측 단말에서 구매자를 인증하는 단계와; 구매자측 단말과 판매자측 단말을 통해 구매자와 임의 판매자의 지문을 공동으로 삽입하는 단계와; 판매자측 단말에서 불법 복사 유무를 검출하여 신뢰기관을 통해 불법 구매자임을 증명하는 단계를 포함하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법을 제공한다.

【발명의 구성 및 작용】

<25> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대해 상세히 설명한다.

<26> 도 1은 본 발명에 따른 방법을 수행하기 위한 핑거프린팅 참여자간의 상호작용 구성도로서, 구매자(100), 판매자(200) 및 신뢰기관(300)을 포함한다. 이때, 각각의 구매자(100), 판매자(200), 신뢰기관(300)은 참여자를 직접 지칭하거나, 참여자측 단말, 예컨대, 데스크탑 또는 노트북으로 가정할 수도 있다.

<27> 도시한 바와 같이, 신뢰기관(300)은 각 참여자가 모두 사용할 수 있는 시스템 매개변수를 생성 및 공개하고, 각 참여자의 공개키와 비밀키를 생성하여 안전한 채널로 제공하는 역할을 담당한다.

<28> 또한, 신뢰기관(300)은 구매자(100)가 판매자(200)에게 자신을 인증하기 위해서 사용되는 인증서를 구매자(100)에게 발행하며, 판매자(200)가 불법 구매자를 검출하여 증거를 제시하는 경우 불법 구매자를 판별하는 과정에 참여한다.

<29> 구매자(100)는 신뢰기관(300)으로부터 제공되는 시스템 매개변수에 따른 공개키와 비밀키를 사용하여 신뢰기관(300)에 구매자 정보(예컨대, 신상 정보 등)를 등록하며, 신뢰기관(300)으로부터 제공되는 값과 자신의 익명 공개키를 사용하여 판매자(200)와의 인증 과정을 수행한다.

<30> 판매자(200)와의 인증 과정에 의해 구매자(100)가 정당한 구매자인 것으로 판단되면, 구매자(100)는 판매자(200)와 대화식 프로토콜을 통해 자신의 신분을 숨긴 채 고유 정보인 지문을 삽입하는 과정에 참여한다.

<31> 판매자(200)는 구매자(100)가 자신을 인증하기 위해 제시하는 값을 검증하여 정당한 구매자인지를 검증하며, 구매자(100)와 공동으로 지문 삽입 과정에 참여하한다.

<32> 이러한 지문 삽입 과정으로부터 불법 구매자를 검출한 경우, 검출한 정보를 이용하여 신뢰기관(300)에 불법 구매자임을 증명할 수 있다.

<33> 이하, 상술한 구성과 함께, 본 발명의 바람직한 실시예에 따른 익명 핑거프린팅 과정을 첨부한 도 2의 흐름도를 참조하여 상세히 설명하기로 한다.

<34> 먼저, 본 과정은, 시스템 매개변수, 구매자(100)의 공개키 및 비밀키 생성 단계(S202)와, 구매자(100)와 신뢰기관(300)간의 정보 등록 단계(S204)와, 판매자(200)에 의한 구매자(100) 인증 단계(S206)와, 구매자(100)와 판매자(200)간의 지문 삽입 단계(S208)와, 판매자(200)와 신뢰기관(300)간의 불법 구매자 판별 단계(S210)와, 신뢰기관(300)이 판매자(200)가 증명하는 불법 구매자를 최종 확인하는 단계(S212)를 포함한다.

<35> 도 2에 도시한 바와 같이, 시스템 매개변수 생성 단계(S202)는, 구매자(100)와 판매자(200) 모두가 공유하는 시스템 매개변수들이 신뢰기관(300)에 의해서 생성되어 공개되는 과정으로서, 이 과정에서 임의의 순환군 G_1과 G_2(이때, G_1과 G_2의 위수는 모두 m)가 생성된다.

<36> 순환군 G_1, G_2가 생성되면, 순환국 G_1의 임의의 생성자 P를 생성하고, 하기 [수학식 1]과 같은 두 순환군에 대한 겹선형 사상을 생성한다.

<37> [수학식 1]

<38> $$e:G_1\times G_1\mapsto G_2$$

<39> 본 발명에서 G_1은 타원곡선군이며, G_2는 Z_m^*와 같은 곱셈 순환군을 사용한다. 신뢰기관(300)은 구매자(100)의 비밀키로 G_2에 속하는 임의의 난수들 s_1, s_2, s_3를 선택하고 비밀키로 설정한 후, 하기 [수학식 2]를 사용하여 구매자(100)의 공개키를 계산한다.

<40> [수학식 2]

<41> $$yB=e(P,P)^{s_1s_2s_3}$$

<42> 그 다음, 구매자 등록 과정(S204)은, 도 3a에 도시한 바와 같다.

<43> 먼저, 단계(S302)에서는, 신뢰기관(300)이 공개한 시스템 매개변수를 바탕으로 G_2에 속하는 임의의 난수 x_R을 생성하여 하기 [수학식 3]에 의해 계산된 값을 구매자(100)에게 전송한다.

<44> [수학식 3]

<45> $$T_R = x_R P$$

<46> 이후, 단계(S304)에서 구매자(100)는 자신의 비밀키를 사용하여 하기 [수학식 4] 및 [수학식 5]를 통해 자신의 익명 공개키 값을 계산하고, 계산된 익명 공개키 값을 신뢰기관(300)에 전송한다.

<47> [수학식 4]

<48> $$X = s_1 s_2 P$$

<49> [수학식 5]

<50> $$Y = s_1 s_2 s_3 P + T_R$$

<51> 익명 공개키 값 X,Y가 신뢰기관(300)에 전송되면, 신뢰기관(300)은 단계(S306)에서와 같이 하기 [수학식 6]을 통해 익명 공개키의 정당성을 검증한다.

<52> [수학식 6]

<53> $$e(X,P) = y_B \cdot e(P,T_R)$$

<54> 신뢰기관(300)에 의해 정당성이 검증되면, 신뢰기관(300)은 하기 [수학식 7]을 통해 T 값을 계산한 후, 인증서 Cert(T), Cert(Y | x_R)을 구매자(100)에게 전송한다.

<55> [수학식 7]

<56> $T=e(X,T_R)$

<57> 구매자(100)가 신뢰기관(300)으로부터 인증서를 받으면, 구매자(100)는 단계(S308)로 진행하여 상술한 [수학식 7]을 통해 정당성을 검증하고, T, Y를 안전하게 보관한다.

<58> 그 다음, 판매자(200)가 구매자(100)를 인증하는 과정(S206)은 도 3b에 도시한 바와 같다.

<59> 먼저, 단계(S402)에서는 구매자(100)가 판매자(200)에게 Y, [T, Cert(T)], 구매정보 text를 전송한다.

<60> 그리고, 구매자(100)는 단계(S404)에서와 같이 G_2에 속하는 임의의 난수 k를 선택한 다음, 하기 [수학식 8]을 통해 text에 대한 서명을 생성한다.

<61> [수학식 8]

<62> $sig=Sign(text,s_1,s_2,s_3,x_R,k)$

<63> 이후, 판매자(200)는 단계(S406)로 진행하여 인증서 Cert(T)를 검증하고, 검증 결과 정당성이 입증된 경우에는 [T, Cert(T)]를 저장한다.

<64> 그 다음, 구매자(100)와 판매자(200)간의 지문 삽입 과정(S208)은 도 3c에 도시한 바와 같다. 이때, 이러한 지문 삽입 과정은 2자간 연산(two-party computation) 기법을 통해 구현될 수 있을 것이다.

<65> 먼저, 단계(S502)에서와 같이 구매자(100)가 x_R, sig, s_1, s_2, Cert(Y $|x_R$)을 판매자(200)에게 전송하면, 판매자(200)는 단계(S504)로 진행하여 T, Y, text, em을 구매자(100)에게 제시한다.

<66> 이러한 값에 기반하여 구매자(100)는 하기 [수학식 9]를 통해 val_1을 계산하여 판매자(200)에게 제시한다(S506).

<67> [수학식 9]

<68> $$val_1 = Verify_1(text, sig, Y)$$

<69> 또한, 구매자(100)는 하기 [수학식 10]을 통해 val_2를 계산하여 판매자(200)에게 제시한다(S508).

<70> [수학식 10]

<71> $$val_2 = Verify_2(Y, Cert(Y \mid x_R), s_1, s_2, x_R, T)$$

<72> 이후, 판매자(200)는 단계(S510)로 진행하여 하기 [수학식 11]과 같은 emb 값을 생성한다.

<73> [수학식 11]

<74> $$emb = text \mid sig \mid Y \mid Cert(Y \mid x_R) \mid s_1 \mid s_2 \mid x_R \mid T$$

<75> 그리고, 이러한 emb 값을 하기 [수학식 12]에 대입하여 삽입된 제품 정보 em*를 계산하여 구매자(100)에게 전송한다.

<76> [수학식 12]

<77> $$em^* = Fing(em, emb)$$

<78> 그 다음, 판매자(200)와 신뢰기관(300)간의 불법 구매자 판별 과정(S210)은 도 3d에 도시한 바와 같다.

<79> 먼저, 단계(S602)에서 판매자(200)는, 익명 공개키 Y를 사용하여 구매정보 text에 대한 서명 sig를 검증한다.

<80> x_R은 상술한 [수학식 5]와 [수학식 7]에 의해서 T, Y와 연결된다. 즉, x_R은 익명 공개키 Y의 소유자가 T의 소유자와 같음을 증명하는데, 신뢰기관(300)만이 구매자(100)에게 [수학식 7]과 하기 [수학식 13]이 동일한 값을 출력하도록 하는 x_R을 제공하기 때문이다.

<81> [수학식 13]

<82> $$T=e(s_1 s_2 P, x_R P)$$

<83> 이후, 판매자(200)는 단계(S604)에서와 같이, 하기 [수학식 14]를 만족하는 공개키의 소유자를 검사한다.

<84> [수학식 14]

<85> $$e(Y,P)=y_B \cdot e(P,P)^{x_R}$$

<86> 단계(S604)에서의 검사 결과, [수학식 14]를 만족하는 경우에는, 신뢰기관(300)을 통해 해당 구매자를 불법 구매자로 증명할 수 있다(S606).

<87> 이상과 같이, 본 발명에 따른 익명 핑거프린팅 기법을 이용하면, 구매자는 자신의 익명성을 유지하면서 원하는 정보에 지문을 안전하게 삽입할 수 있으며, 판매자는 불법 복사나 불법 배포가 검출된 경우 검출한 정보를 바탕으로 신뢰기관을 통해 불법 구매자를 증명할 수 있다.

<88> 또한, 본 발명은 무선 통신과 같은 환경에서 구매자의 연산 능력이 뒤떨어지는 상황을 고려하여 키 크기를 줄여 전체 연산의 효율성을 극대화하였다. 이러한 키 크기의 감소는 타원곡선 암호 시스템의 장점에 근거한 것으로, 그 구체적인 기술 내용은 본 발명의 기술 분야에서 통상의 지식을 가진 자라면 용이하게 알 수 있을 것이다.

【발명의 효과】

<89> 본 발명은 겹선형쌍을 사용하여 안전한 익명 핑거프린팅 기법을 제공할 수 있다.

<90> 인터넷의 급속한 발전에 따라 전자 상거래가 활발해지면서, 디지털 정보에 대한 지적 소유권의 보호가 필수적으로 요구되고 있는 즈음에, 본 발명은 기존의 대칭 핑거프린팅 기법이나 비대칭 핑거프린팅 기법의 단점을 해결할 뿐만 아니라, 겹선형쌍을 사용하여 연산 과정을 단순화함으로써 기존 익명 핑거프린팅 기법에서의 연산의 비효율성을 최소화하는 효과가 있다.

<91> 특히, 겹선형 사상은 테이트 쌍이나 베일 쌍을 타원곡선 상에서 구현하여 사용하였다. 이때, 테이트 쌍이나 베일 쌍의 계산이 상대적으로 복잡하여 연산의 비효율성이 지적될 수 있으나, 현재 암호학자들의 지속적인 연구로 인하여 연산 시간 개선이 꾸준이 이루어지고 있으며, 최근에는 계산량을 줄이는 알고리즘의 연구에 힘입어 테이트 쌍이나 베일 쌍의 연산도 매우 효율적으로 계산되고 있다.

<92> 이상, 본 발명을 실시예에 근거하여 구체적으로 설명하였지만, 본 발명은 이러한 실시예에 한정되는 것이 아니라, 하기 특허청구범위의 요지를 벗어나지 않는 범위내에서 여러 가지 변형이 가능한 것을 물론이다.

【특허청구범위】

【청구항 1】

구매자, 판매자 및 신뢰기관을 포함하는 참여자 또는 참여자측 단말을 네트워크를 통해 연결하는 익명 핑거프린팅(Fingerprinting) 방법에 있어서,

상기 신뢰기관을 통해 상기 구매자 및 판매자를 공유하는 겹선형 사상($e:G_1\times G_1\mapsto G_2$)을 만족하는 시스템 매개변수($G_1$, G_2, m, P, e : 상기 m은 위수, 상기 G_1은 상기 m의 타원곡선군, 상기 G_2는 상기 m의 곱셈 순환군, 상기 P는 상기 G_1의 생성자)를 생성 및 공개하는 제 1 단계와;

상기 신뢰기관을 통해 상기 G_2에 속하는 임의의 난수를 선택하여 상기 구매자의 비밀키(s_1,s_2,s_3)로 설정한 후, 상기 구매자의 공개키($y_B = e(P,P)^{s_1 s_2 s_3}$)를 계산하는 제 2 단계와;

상기 신뢰기관을 통해 공개된 시스템 매개변수, 비밀키 및 공개키를 바탕으로 상기 구매자와 상기 신뢰기관간의 정보를 등록하는 제 3 단계와;

상기 구매자의 정보를 바탕으로 상기 판매자가 상기 구매자를 인증하는 제 4 단계와;

상기 구매자와 상기 판매자의 지문 정보를 상호 삽입하는 제 5 단계와;

상기 신뢰기관을 통해 검출된 시스템 매개변수, 비밀키, 공개키 정보와, 상기 판매자를 통해 검출된 상기 구매자의 지문 정보를 바탕으로 상기 판매자와 상기 신뢰기관간의 불법 복사 및 불법 구매자를 판별하는 제 6 단계와;

상기 신뢰기관이 상기 판매자가 증명하는 불법 구매자를 최종 확인하는 제 7 단계를 포함하는 네트워크상에서의 겹선형쌍 디피-헬만 문제(Bilinear Diffie-Hellman Problem)를 이용한 익명 핑거프린팅 방법.

【청구항 2】

제 1 항에 있어서,

상기 제 3 단계는,

상기 신뢰기관이 상기 G_2에 속하는 임의의 난수(x_R)를 생성하여 계산된 값($T_R=x_RP$)을 상기 구매자에게 전송하는 단계와;

상기 구매자가 상기 비밀키를 사용하여 계산된 익명 공개키 값($X=s_1s_2P$, $Y=s_1s_2s_3P+T_R$)을 상기 신뢰기관에 전송하는 단계와;

상기 신뢰기관에서 제 1 검증식($e(X,P)=y_B \cdot e(P,T_R)$)을 이용하여 상기 익명 공개키(X,Y)의 정당성을 검증하는 단계와;

상기 신뢰기관에 의해 상기 익명 공개키의 정당성 검증이 완료되면, 상기 신뢰기관에서 제 2 검증식($T=e(X,T_R)$)을 계산한 후 인증서(Cert(T), Cert(Y | x_R))를 발행하여 상기 구매자에게 전송하는 단계와;

상기 구매자가 상기 제 2 검증식($T=e(X,T_R)$)을 통해 정당성을 검증하고 상기 난수(x_R), 상기 제 2 검증식(T), 상기 익명 공개키(Y)를 보관하는 단계로 이루어지는 것을 특징으로 하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 제 4 단계는,

상기 구매자에서 상기 판매자로 상기 익명 공개키(Y), 상기 제 2 검증식(T), 상기 인증서(Cert(T)), 구매정보(text)를 전송하는 단계와;

상기 구매자에서 상기 G_2에 속하는 임의의 난수 k를 생성한 후 상기 구매정보(text)에 대한 서명($sig=Sign(text,s_1,s_2,s_3,x_R,k)$)을 생성하는 단계와;

상기 판매자에서 상기 인증서(Cert(T))를 검증하고, 정당성이 입증된 경우 상기 T, 상기 인증서(Cert(T))를 저장하는 단계로 이루어지는 것을 특징으로 하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법.

【청구항 4】

제 1 항 또는 제 2 항에 있어서,

상기 제 5 단계는,

상기 구매자가 난수(x_R, s_1, s_2), 서명(sig), 상기 인증서(Cert(Y | x_R))를 상기 판매자에게 전송하는 단계와;

상기 판매자가 상기 익명 공개키(Y), 상기 제 2 검증식(T), 구매정보(text), 제품정보(em)를 상기 구매자에게 전송하는 단계와;

상기 구매자가 $val_1=Verify_1(text, sig, Y)$ 및 $val_2=Verify_2(Y,Cert(Y \mid x_R), s_1, s_2, x_R, T)$을 계산하여 상기 판매자에게 전송하는 단계와;

상기 판매자가 제품정보(emb=text | sig | Y | Cert(Y | x_R) | s_1 | s_2 | x_R | T) 및 지문이 삽입된 제품정보(em*=Fing(em, emb))를 생성하여 상기 구매자에게 전송하는 단계로 이루어지는 것을 특징으로 하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법.

【청구항 5】

제 4 항에 있어서,

상기 제 5 단계는 2자간 연산(two-party computation) 기법에 의해 구현되는 것을 특징으로 하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법.

【청구항 6】

제 1 항 또는 제 2 항에 있어서,

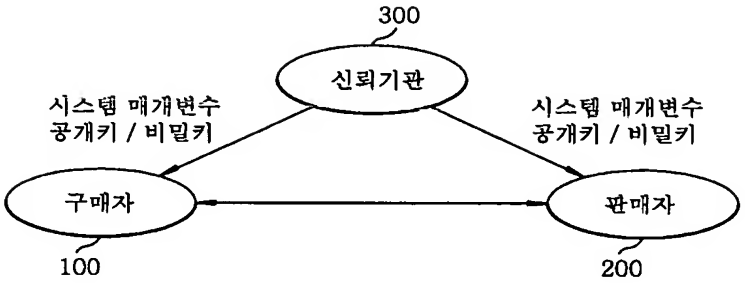
상기 제 6 단계는,

상기 판매자가 상기 익명 공개키(Y)를 사용하여 구매정보(text)에 대한 서명(sig)을 검증하는 단계와;

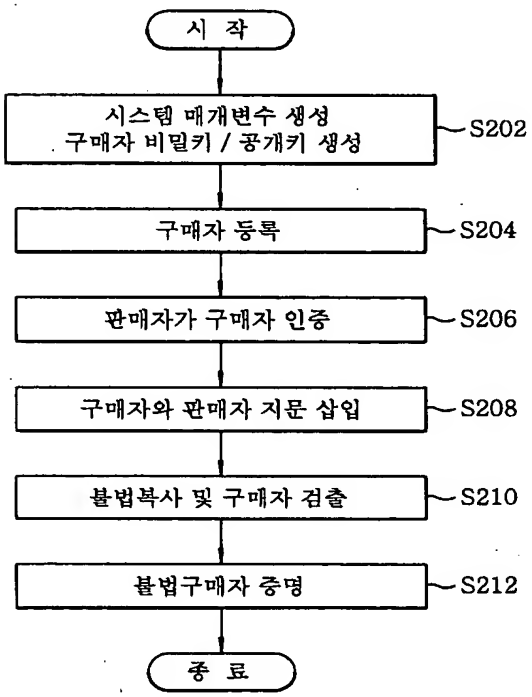
상기 판매자가 수학식($e(Y,P)=y_B \cdot e(P,P)^{x_R}$)을 만족하는 공개키의 소유자를 불법 구매자로 판정하는 단계로 이루어지는 것을 특징으로 하는 네트워크상에서의 겹선형쌍 디피-헬만 문제를 이용한 익명 핑거프린팅 방법.

【도면】

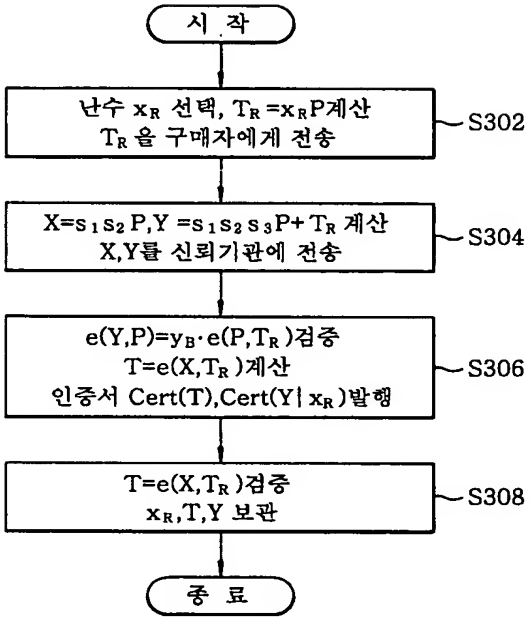
【도 1】


300
신뢰기관
시스템 매개변수
공개키 / 비밀키
시스템 매개변수
공개키 / 비밀키
구매자
판매자
100
200

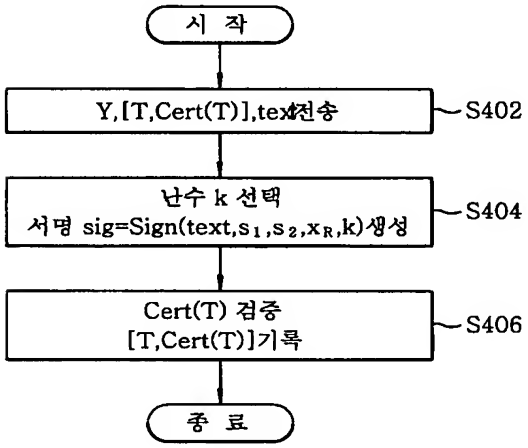
【도 2】


시 작
시스템 매개변수 생성
구매자 비밀키 / 공개키 생성
S202
구매자 등록
S204
판매자가 구매자 인증
S206
구매자와 판매자 지문 삽입
S208
불법복사 및 구매자 검출
S210
불법구매자 증명
S212
종 료

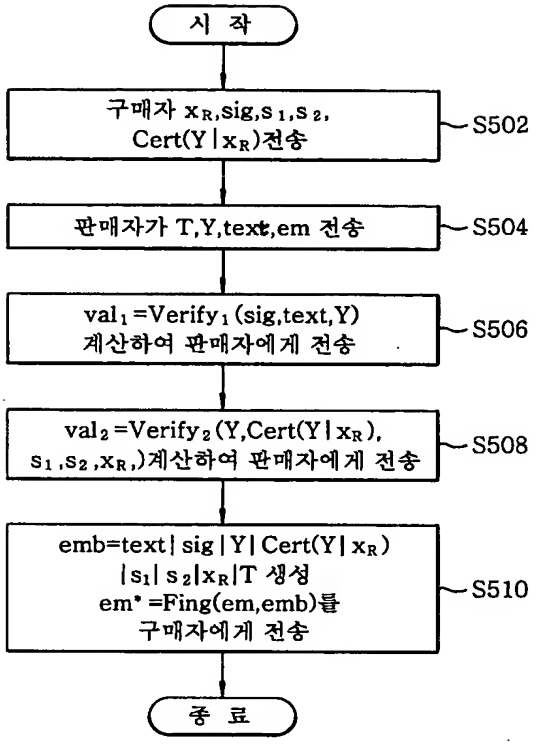
【도 3a】


시 작
난수 x_R 선택, $T_R = x_R P$계산
T_R 을 구매자에게 전송
S302
$X = s_1 s_2 P, Y = s_1 s_2 s_3 P + T_R$ 계산
X,Y를 신뢰기관에 전송
S304
$e(Y,P) = y_B \cdot e(P,T_R)$검증
$T = e(X,T_R)$계산
인증서 Cert(T),Cert(Y| x_R)발행
S306
$T = e(X,T_R)$검증
x_R,T,Y 보관
S308
종 료

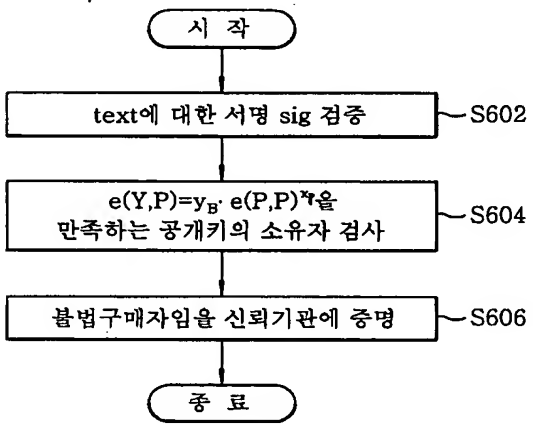
【도 3b】


시 작
Y,[T,Cert(T)],text전송
S402
난수 k 선택
서명 sig=Sign(text,s_1,s_2,x_R,k)생성
S404
Cert(T) 검증
[T,Cert(T)]기록
S406
종 료

【도 3c】


시 작
구매자 x_R,sig,s_1,s_2, Cert(Y|x_R)전송
S502
판매자가 T,Y,text,em 전송
S504
val_1 =$Verify_1$ (sig,text,Y) 계산하여 판매자에게 전송
S506
val_2 =$Verify_2$(Y,Cert(Y|x_R), s_1,s_2,x_R,)계산하여 판매자에게 전송
S508
emb=text|sig|Y|Cert(Y|x_R) |s_1|s_2|x_R|T 생성 em* =Fing(em,emb)를 구매자에게 전송
S510
종 료

【도 3d】


시 작
text에 대한 서명 sig 검증
S602
e(Y,P)=y_B· e(P,P)^{x_B}을 만족하는 공개키의 소유자 검사
S604
불법구매자임을 신뢰기관에 증명
S606
종 료